CPNI Compliance Policies of

The City of Albany Utility Board/Water, Gas & Light Commission

The City of Albany Utility Board , Water, Gas & Light Commission ("Albany"), a public utility established by City Charter of the City of Albany, Georgia has implemented the following policies and procedures to protect the confidentiality of Customer Proprietary Network Information ("CPNI') and to assure compliance with the rules of the Federal Communications Commission ("FCC") set forth in 47 C. F. R. Part 64, Subpart U, Section 2001 et seq., including the FCC's new rules adopted in *Implementation of the Telecommunications Act of 1996: Telecommunications Carriers' Use of Customer Proprietary Network Information and Other Customer Information,* CC Docket No. 96-11, Report and Order and Further Notice of Proposed Rulemaking, FCC 07-22 (rel. April 2, 2007).

CPNI is "(A) information that relates to the quantity, technical configuration, type, destination, location, and amount of use of a telecommunications service subscribed to by any customer of a telecommunications carrier, and that is made available to the carrier by the customer solely by virtue of the carrier-customer relationship; and (B) information contained in the bills pertaining to telephone exchange service or telephone toll service received by a customer of a carrier."

Albany's policy is administered by its CPNI Compliance Manager Jimmy Norman, its Director of Utility Construction.

I. USE, DISCLOSURE OF, AND ACCESS TO CPNI

Albany may use, disclose, or permit access to CPNI only in its provision of the communications service from which such information is derived; for services necessary to, or used in, the provision of such communications service, including to initiate, render, bill and collect for telecommunications services; to protect users or other carriers or service providers from fraudulent, abusive or unlawful use of, or subscription to, such services; to provide installation, maintenance, or repair services; as required by law; or as expressly authorized by the customer.

Albany does not use, disclose or permit access to CPNI to identify or track customers that call competing service providers.

Albany does not use CPNI to market its services. In the event that any employee wishes to use CPNI for marketing or to seek customer approval for such use, such proposed use would be subject to a supervisory review process that shall involve the CPNI Compliance Manager. If such use is approved, Albany shall modify these policies and conduct additional training as needed to assure compliance with the FCC's rules.

In accordance with Section 222(b) of the Act, 47 U.S.C. § 222(b), when Albany receives or obtains proprietary information from another carrier for purposes of providing a telecommunications service, it only uses such information for such purpose, and does not use such information for its own marketing efforts.

II. SAFEGUARDS AGAINST DISCLOSURE OF CPNI TO UNAUTHORIZED PARTIES

Albany will take reasonable measures to discover and protect against attempts to gain unauthorized access to CPNI. If any employee becomes aware of new methods that are being used or could be used by third parties to attempt to obtain unauthorized access to CPNI, or of possible changes to Albany's existing policies that would strengthen protection of CPNI, they should report such information immediately to Albany's CPNI Compliance Manager so that Albany may evaluate whether existing policies should be supplemented or changed.

Albany does not disclose, Call Detail Information to any inbound telephone caller or any visitor to an Albany retail office, and does not provide online access to any account that provides access to CPNI. Albany's representatives with access to CPNI have a personal relationship with all of Albany's customers, and do not disclose other types of CPNI to an inbound caller without authenticating the caller as the customer using an authentication method that is appropriate for the information sought and which adheres to Albany's duty to protect CPNI. Albany may disclose a customer's CPNI to authorized person visiting an Albany Office upon verifying through a valid, non-expired government-issued photo ID (such as a driver's license, passport, or comparable ID) that the person is authorized to receive such information. When a customer's address of record is created or changed, except when customer initiates service, Albany will send a notice immediately to customer's preexisting address of record notifying them of the change. These notifications will not reveal the changed information.

Pursuant to 47 C.F.R. § 64.201(g), the requirements of the FCC's authentication regime set forth in the preceding paragraph do not apply to business customer accounts where the business customer has a dedicated account representative (that may be reached without going through a call center) and a contract with Albany that specifically addresses Albany's protection of CPNI.

III. REPORTING CPNI BREACHES TO LAW ENFORCEMENT

Any Albany employee that becomes aware of any breaches, suspected breaches or attempted breaches must report such information immediately to the Albany CPNI Compliance Manager, and such information must not be reported or disclosed by any employee to any non-employee, including the potentially affected customer, except in express conformance with the procedures described below. Any employee that fails to report such information will be subject to disciplinary action that may include termination.

It is Albany's policy that employees should not be discouraged from reporting information about breaches that may have been caused in part by their own actions or omissions. Once a breach has occurred, the most important objective is to attempt to limit the damage to customers, make any adjustments as needed to prevent a recurrence of the breach, and to alert law enforcement promptly. Therefore, although employees who violate Albany's CPNI compliance procedures are subject to discipline, the sanctions may be substantially reduced where employees promptly self-report violations if appropriate.

Nothing in this policy authorizes any employee to violate Georgia law. In the event of an apparent conflict between Georgia law and the FCC's CPNI requirements or the requirements of this policy, the Albany CPNI Compliance Manager will consult the Albany's legal counsel.

A. Identifying a "Breach"

A "breach" has occurred when a person, without authorization or exceeding authorization, has intentionally gained access to, used, or disclosed CPNI. If an employee has information about an incident and is not certain that the incident would not constitute a breach under this definition, the incident must be reported to the CPNI Compliance Manager.

If an Albany employee determines that an unauthorized person is attempting to gain access to CPNI but does not succeed at doing so, no breach has occurred. However, the incident must be reported to Albany's CPNI Compliance Manager who will determine whether to report the incident to law enforcement and/or take other appropriate action. Albany's CPNI Compliance Manager will determine whether it is appropriate to update Albany's CPNI policies or training materials in light of any new information; the FCC's rules require Albany on an ongoing basis to "take reasonable measures to discover and protect against activity that is indicative of pretexting."

B. Notification Procedures

As soon as practicable, and in no event later than 7 business days upon learning of a breach, the Albany CNI Compliance Manager shall electronically notify the United States Secret Service (USSS) and the Federal Bureau of Investigation (FBI) by accessing the following link: https://www.cpnireporting.gov. Albany's FRN number and password may be required to submit a report. If this link is not responsive, they should contact counsel or the FCC's Enforcement Bureau (202-418-7450 or http://www.fcc.gov/ob/cpni) for instructions.

Albany will not notify customers or disclose a breach to the public until 7 full business days have passed after notification to the USSS and the FBI, except as provided below (a full business day does not count a business day on which the notice was provided). If Albany receives no response from law enforcement after the 7th full business day, it must promptly proceed to inform the customers whose CPNI was disclosed of the breach.

Albany will delay notification to customers or the public upon request of the FBI or USSS.

If the Albany Compliance Manage believes there is a need to disclose a breach sooner, he or she should so indicate in the notification to law enforcement. However, such notification does not itself permit notice to customer; Albany still may not notify customers sooner unless given clearance to do so from both the USSS and the FBI.

IV. RECORD RETENTION

The CPNI Compliance Manager is responsible for assuring that Albany maintains for at least two years a record, electronically or in some other manner, of any breaches discovered, notifications made to the USSS and the FBI pursuant to these procedures, and notifications of breaches made to customers. The record must include, if available, dates of discovery and notifications, a detailed description of the CPNI that was the subject of the breach, and the circumstances of the breach.

Albany maintains a record, for a period of at least one year, of those limited circumstances in which CPNI is disclosed or provided to third parties, or where third parties were allowed access to CPNI.

Because Albany does not use CPNI for marketing or for any other purpose for which customer approval is required, it does not have any records to keep regarding supervisory review of marketing; or of sales and marketing campaigns that use CPNI; or of records associated with customers' approval or non-approval to use CPNI, or notification to customers prior to any solicitation for customer approval to use or disclose CPNI.

Albany will maintain a record of any customer complaints related to their handling of CPNI, and records of Albany's handling of such complaints, for at least two years. The CPNI Compliance Manager will assure that all complaints are reviewed and that Albany considers any necessary changes to its policies or practices to address the concerns raised by such complaints.

Albany will have an officer, as its authorized agent, sign a compliance certificate on an annual basis stating personal knowledge that Albany has established operating procedures that are adequate to ensure its compliance with FCC's Enforcement Bureau in EB Docket No. 06-36 by March 1 of the subsequent year, and will be accompanied by a summary or copy of this policy that explains how Albany's operating procedures ensure that it is in compliance with the FCC's CPNI rules. In addition, the filing must include an explanation of any actions taken against data brokers and a summary of all customer complaints received in the past year concerning the unauthorized release of CPNI. Any confidential portions of these submissions shall be redacted from the public version of the filing and provided only to the FCC.

V. TRAINING

All employees with access to CPNI receive a summary of Albany's CPNI policies and are informed that (i) any use or disclosure of CPNI or other act or omission not in compliance with such policies will result in disciplinary action, including the termination of employment where appropriate, and (ii) employees who knowingly facilitate the unauthorized disclosure of a customer's confidential information may be subject to criminal penalties.